Journal of Criminal Law and Criminology

Volume 102 | Issue 1 Article 8

Winter 2012

The Data-Broker Threat: Proposing Federal Legislation to Protect Post-Expungement Privacy

Logan Danielle Wayne

0091-4169/12/10201-0253
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 102, No. 1

THE DATA-BROKER THREAT: PROPOSING FEDERAL LEGISLATION TO PROTECT POST-EXPUNGEMENT PRIVACY

Logan Danielle Wayne*

I. INTRODUCTION

Imagine if you will the following hypothetical: An eighteen-year-old who recently graduated from high school is arrested in California for possession of marijuana. Under California state law, possession of not more than 28.5 grams of marijuana is classified as an infraction and carries a maximum punishment of a $100 fine.[1] The young man pleads guilty and timely pays all fines and court fees. Two years later, in accordance with state law, the court destroys any records pertaining to the young man's arrest and conviction.[2] However, in the interim a company called DataBrokerX purchased electronic records from the jurisdiction that was holding the young man's file, including records of the young man's arrest and guilty plea. Once DataBrokerX purchases the records, it stores the information in its private database.[3] Several years later, the young man graduates from college and, without having any other run-ins with the law, applies for his first job. The employer runs a background check through DataBrokerX and the young man is not selected for the position because the conviction appears on that consumer report. The employer would never know that the conviction was vacated because DataBrokerX obtained the young man's records before the state granted the expungement.[4] Also, the

* J.D. Candidate, Northwestern University School of Law, 2012.

[1] CAL. HEALTH & SAFETY CODE § 11357 (West 2007 & Supp. 2011).

[2] CAL. HEALTH & SAFETY CODE § 11361.5 (West 2007) (providing that all convictions and arrests under § 11357(b) shall not be kept longer than two years after the date of conviction, or two years after the date of arrest for arrests not resulting in convictions, and that any court or agency having custody of the records shall destroy the records at that time).

[3] *See infra* Part III for a discussion of the data-broker industry. "Data broker" refers generally to private background check companies and, as used in this Comment, refers to those companies that provide information about criminal records obtained from local courts or other public records sources.

[4] The term "expungement," as used herein, refers to the full range of remedies that allow for the sealing, purging, or erasure of a criminal conviction.

young man may never find out why he was denied employment because employers are not required to tell potential employees why they were denied a job.[5] Finally, even if the young man is informed that it was due to his criminal conviction, this is of little consolation as he has already suffered by losing the job opportunity. This is precisely the type of injury that expungements are designed to prevent.[6] But, despite the court's expungement of this young man's record to prevent further lost opportunities, the young man must go through steps to remove the information from DataBrokerX's archives.[7] Once he has done this, there is still no guarantee that DataBrokerX is the only company with the information.

It is a reasonable argument that a young man in this position deserves a second chance. However, even barring debate about whether or not the young man deserved to have his conviction expunged, one can recognize that once the young man has been granted an expungement, he is entitled by law to the benefits of that expungement. It is a fundamental principle of our legal system that the law must be upheld. This Comment will argue that, once an expungement is granted, it is wrong for a non-governmental source to release information about the conviction, because that action undermines the purpose of expungement laws.

Expungement is a special form of relief that allows individuals, like the young man in the hypothetical, to "restore him[self] to his former status in society"[8] by essentially erasing his criminal history and granting him a clean slate. This allows individuals with expunged records to legally

---

[5] One major problem with the issue proposed herein is that it is difficult, if not impossible, to determine how often expunged records are released or how often the release of expunged records results in the loss of housing or an employment opportunity. This is due, in part, to the fact that employers are not required to disclose why they pass over a particular person for a job and landlords do not have to disclose why they choose one tenant over another. As such, there is currently no way of determining precisely how many people are affected by the wrongful dissemination of expunged records. This Comment is somewhat limited due to that lack of empirical research to back up its claims; however, the fact that the structure of the data-broker industry allows for the release of expunged criminal records combined with reports of individual incidents where expunged records have been wrongfully released, provide enough of a basis for the arguments contained herein. An interesting and important supplement to this Comment would be an empirical study quantifying the effect of the data-broker industry on post-expungement privacy. *See infra* Part III for further discussion.

[6] *See infra* Part II.

[7] Removing information from a data broker's archive is often an arduous process that can even require a person to purchase his or her own records before requesting that the information be removed. *See infra* note 80 and accompanying text.

[8] People v. Mgebrov, 82 Cal. Rptr. 3d 778, 781 (Cal. Ct. App. 2008). Other state courts have described the purpose for providing expungement in similar terms. *See infra* Part II.

refrain from disclosing information about their expunged conviction to potential employers or landlords.[9] When the expungement is granted, an expungement order is served on a government recordkeeping agency; this order generally requires the destruction or prohibits the release of any records pertaining to the expunged arrest or conviction.[10] However, because trials are public and criminal information is also a matter of public record, it is currently not illegal for non-government sources (e.g., data brokers) to obtain criminal records.[11] Furthermore, expungement orders do not apply to non-government sources.[12] This may be because when expungement laws were first passed, the government was the only source for obtaining criminal records,[13] or perhaps because legislators did not predict the growth of the data-broker industry. Either way, data brokers are currently free to distribute information from expunged records without any repercussions.

Having identified a pertinent example of how technology has outpaced regulation, this Comment proposes that a massive and largely unregulated private data-broker industry poses a significant threat to post-expungement privacy at potentially great cost to individuals with expunged records.[14] Data brokers are not required to update their records, and as a result, expunged convictions are being released to the public through these private companies.[15]

Currently the onus of enforcing postconviction privacy rights is on individuals with expunged records.[16] This Comment will propose that, because of the digitization of data sharing and the increased prevalence of the data-broker industry, individual enforcement is ineffective if not helpless to protect the rights of individuals with expunged records. Ultimately, this Comment will argue that if such violations of post-

---

[9] *See infra* Part II.

[10] *See* SEARCH, NAT'L CONSORTIUM FOR JUSTICE INFO. & STATISTICS, REPORT OF THE NATIONAL TASK FORCE ON THE COMMERCIAL SALE OF CRIMINAL JUSTICE RECORD INFORMATION 82–83 (2005), *available at* http://www.search.org/files/pdf/RNTFCSCJRI.pdf. [hereinafter SEARCH REPORT].

[11] *See infra* Part III.

[12] SEARCH REPORT, *supra* note 10, at 83.

[13] *See infra* Part III.

[14] *See, e.g.*, Adam Liptak, *Criminal Records Erased by Courts Live to Tell Tales*, N.Y. TIMES, Oct. 17, 2006, at A1.

[15] *Id.*; *see also* Rebecca Oyama, Note, *Do Not (Re)Enter: The Rise of Criminal Background Tenant Screening as a Violation of the Fair Housing Act*, 15 MICH. J. RACE & L. 181, 188–89 (2009).

[16] Oyama, *supra* note 15, at 189; *see also* SEARCH REPORT, *infra* note 76 (discussing the process for removing records from proprietary databases).

expungement privacy continue unregulated, they have the potential to render the legal remedy of expungement moot in the real world.[17] Therefore, because of the potential magnitude of this problem, an ex ante remedy in the form of federal legislation is the only way to protect post-expungement privacy rights and expungement law itself. As such, this Comment proposes goals for a federal statutory scheme.[18]

This Comment will proceed in four major parts. Part II discusses the underlying purpose for and importance of providing relief through expungement.[19] Of particular importance is that expungement allows individuals to obtain employment and housing, unhampered by their status as ex-offenders. Part III proceeds by discussing the evolution of the data-broker industry and how criminal records have become readily available through largely unregulated, private, non-government sources. Part III argues that the unregulated release of information by data brokers is posing a serious threat to the important role that expungement plays. Part IV discusses why a federal regulatory scheme is the best way to protect post-

---

[17] For a discussion on the importance of expungement as a legal remedy, see *infra* Part II.

[18] A major issue that often arises in the context of expungement is policy concerns about allowing ex-offenders to conduct themselves in society unidentified as having been convicted of a crime. James W. Diehm, *Federal Expungement: A Concept in Need of a Definition*, 66 ST. JOHN'S L. REV. 73, 75–80 (1992). Although such policy concerns do play a significant part in the overall scope of expungement scholarship and jurisprudence, they are beyond the scope of this Comment. Because public safety concerns associated with the nondisclosure of an individual's criminal record increase with the severity of the crime, this Comment applies only to those instances where expungement is arguably most uncontroversial: misdemeanor offenses and arrests that do not result in conviction. The intention is to ameliorate policy concerns that account for the differences in expungement laws from state to state. For this reason, juvenile and sex-related expungements are excluded. Furthermore, even though a small percentage of states have passed laws that allow expungement of felony convictions, such statutes are excluded from this analysis because they tend to spark the most heated debate surrounding policy considerations. *E.g.*, ARK. CODE ANN. §§ 16-93-301 to -303 (2006) (permitting expungements for first-time felony convictions unless the crime involved a sex offense with a victim under the age of eighteen); DEL. CODE ANN. tit. 11, § 8506(c) (2007) (providing for expungement of felony convictions once the person reaches age eighty or reaches age seventy-five with no criminal activity listed on the person's record in the preceding forty years); KAN. CRIM. PROC. CODE ANN. § 21-6614 (West, Westlaw through 2010 Legis. Sess.) (allowing expungement for certain felony convictions between three and ten years after completion of sentence, depending on the severity of crime). That being said, the fact that a vast majority of states allow expungement of certain misdemeanor records is evidence that we as a society have embraced the idea that some people deserve a fresh start.

[19] There is currently no federal expungement statute. For a discussion of the need for a federal expungement statute, see Fruqan Mouzon, *Forgive Us Our Trespasses: The Need for Federal Expungement Legislation*, 39 U. MEM. L. REV. 1 (2008).

expungement privacy rights. Finally, this Comment concludes with Part V, outlining the legislative aims in creating such a statute.

II. THE IMPORTANCE OF EXPUNGEMENT AS A LEGAL REMEDY

Offering relief to individuals with expunged records *after* information from the expunged records has been released is about as effective as offering an umbrella after the rain. This is because once a data broker releases the criminal record, the purpose of expungement is significantly undermined. Before delving into violations of post-expungement privacy, this Comment will explore the rights expungement bestows upon a person and the source of those rights are derived. This Part begins with a brief history and overview of expungement, then focuses on the importance of expungement as a form of legal relief and the purpose that it serves in society, and concludes with a discussion about the right to post-expungement privacy and how the protection of information pertaining to expunged convictions is vital to the survival of expungement as a legal remedy.

A. HISTORY AND OVERVIEW

As of 2008, forty-five states and the District of Columbia have some form of expungement legislation.[20] While the remedy has been given many different names—"sealing,"[21] "erasure,"[22] "deferred judgment,"[23] "setting aside,"[24] "vacated"[25]—the general aim behind each individual state law is remarkably similar across jurisdictions. The goal is to eliminate at least some of the collateral consequences associated with criminal convictions and to facilitate reintegration into society for certain individuals by essentially granting them a clean slate.[26]

Expungement is not granted lightly.[27] Especially in the circumstances

---

[20] Mouzon, *supra* note 19, at 31 ("Most states have addressed the expungement issue through legislation. Forty-five states, plus the District of Columbia, provide relief for some ex-offenders from the bondages attached to having a criminal history, either through expungement or other similar relief.") (footnotes omitted).

[21] *See, e.g.*, ALASKA STAT. § 12.62.180 (2006).

[22] *See, e.g.*, CONN. GEN. STAT. ANN. § 54-142a (West 2009 & Supp. 2011).

[23] *See, e.g.*, IOWA CODE ANN. § 907.3 (West 2003 & Supp. 2011).

[24] *See, e.g.*, MICH. COMP. LAWS ANN. § 780.621 (West 2007).

[25] *See, e.g.*, WASH. REV. CODE ANN. §§ 9.94A.640, 9.95.240 (West 2009).

[26] *See infra* Part II.B.

[27] Jon Geffen & Stefanie Letze, *Chained to the Past: An Overview of Criminal Expungement Law in Minnesota*—State v. Schultz, 31 WM. MITCHELL L. REV. 1331, 1335 (2005) ("Expungement is defined at law as an 'extraordinary form of relief.' It does not apply to every individual suffering the detrimental effects of a criminal history . . . . [T]he

to which this Comment is limited, expungement is granted only to those who deserve it most.[28] In sum, this Comment focuses only on misdemeanor convictions and reports of arrests that do not result in conviction—those instances of expungement where it can be assumed that the benefits gained by granting expungement outweigh any potential harms to society and public safety.[29]

B. THE IMPORTANCE OF EXPUNGEMENT

The most basic explanation for expungement is that we, as a society, recognize that some people deserve a second chance.[30] Or, at the very least, our society has recognized that certain offenders do not deserve 'criminal' status once they have paid their debts to society.[31] As such, the fundamental goal of expungement is to provide relief from the stigma associated with criminal status.[32] Our society makes a litany of

---

remedy is unique and given only to the most deserving individuals." (footnote omitted)).

[28] *See infra* Part II.B.

[29] For support of society's interest in granting expungement, see Geffen & Letze, *supra* note 27, at 1340 ("Expungement relieves society of the burden of supporting certain individuals with criminal records. As previously explained, an expungement can allow an individual to obtain employment and eliminate the individual's reliance on government benefits.").

[30] *See, e.g.*, State v. N.W., 747 A.2d 819, 823 (N.J. Super. Ct. App. Div. 2000) (finding the New Jersey legislature's purpose in enacting an expungement statute was to "give a one-time offender who has changed his or her life a second chance"); Steven K. O'Hern, *Expungement: Lies That Can Hurt You In and Out of Court*, 27 WASHBURN L.J. 574, 574 ("Expungement of a prior criminal conviction is often viewed as an admirable process, allowing an ex-offender a fresh start." (footnotes omitted)).

[31] Luz A. Carrion, *Rethinking Expungement of Juvenile Records in Massachusetts: The Case of* Commonwealth v. Gavin G., 38 NEW ENG. L. REV. 331, 368 (referring to both adult and juvenile expungement and stating that "[r]ecord expungement serves the crucial societal function of giving a second chance to the average person who needs a clean record to advance and succeed in life and who will be most harmed by a record's existence" (internal quotation marks omitted)).

[32] Nora V. Demleitner, *Preventing Internal Exile: The Need for Restrictions on Collateral Sentencing Consequences*, 11 STAN. L. & POL'Y REV. 153, 157 (1999) (addressing the effect of collateral consequences and stating that "deprivation of the benefits of citizenship carries a strong symbolic message stigmatizing convicted felons as less than full members of society"); Andrew Hacker, Comment, *The Use of Expunged Records to Impeach Credibility in Arizona*, 42 ARIZ. ST. L.J. 467, 470 (2010) ("The 'collateral consequences' of a criminal record often carry other, more subtle burdens that are not easily quantified. The social stigma associated with a criminal past—sometimes referred to as 'the stigma of conviction'—often is unaffected even after a rehabilitated offender has had his civil rights restored. The simple fact that an offender carries a record serves to 'emphasize [the offender's] "other-ness"' within society." (citing Margaret Colgate Love, *Starting Over with a Clean Slate: In Praise of a Forgotten Section of the Model Penal Code*, 30 FORDHAM URB. L.J. 1705, 1716 (2003))).

assumptions about a person upon learning that they have a criminal record: it is assumed that they are somehow less credible[33] and less trustworthy.[34] Further, important employment and housing decisions can be based solely on ex-offender status.[35]

The conundrum herein is further complicated when knowledge of a criminal conviction is obtained through the use of data brokers. First and foremost, data brokers maintain proprietary databases and most are not required to update their records.[36] This Comment proposes that because of this lack of regulation in updating their records, expunged convictions are stored and released from these proprietary databases as if they had never been expunged.[37] Another problem with information from data brokers is that, in creating consumer reports, data brokers often omit information and reword or misinterpret language from the original court documents.[38] The resulting report might therefore contain a record of an arrest but no record of the disposition—a serious problem if the charges were subsequently dropped, for example.[39] Or a report might mention the same offense twice, when in reality, the individual was only convicted of the offense a single time.[40]

The problem arises because assumptions are made about a person with

---

[33] Even our judicial system allows for the introduction of a person's prior criminal conviction "[f]or the purpose of attacking the character for truthfulness" of that witness. FED. R. EVID. 609.

[34] Mouzon, *supra* note 19, at 2 ("The mere existence of a criminal history can produce assumptions of past dishonesty and future untrustworthiness in the minds of all those aware of that history." (footnote omitted)). *Cf.* Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1056 (2003) (stating that information about a person's criminal past is highly relevant to determining a person's trustworthiness).

[35] Geffen & Letze, *supra* note 27, at 1332 ("A publicly available criminal record is devastating to an individual's hope of re-integrating into society, especially with respect to employment and housing.").

[36] *See infra* Part III.

[37] However, there is a lack of empirical data to support this proposition, so this Comment also advocates the need for an empirical study. *See supra* text accompanying note 5.

[38] For a thorough discussion of the potential problems with electronic databases, see Elizabeth D. De Armond, *Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation*, 41 VAL. U. L. REV. 1061, 1075–96 (2007); *see also* SEARCH REPORT, *supra* note 10, at 11 (describing the process by which data brokers catalogue information in their databases by converting information from many different sources into one standard format that varies from data broker to data broker); *see also* Oyama, *supra* note 15, at 188–90 (noting that commercial criminal records databases are often "rife with error," resulting in inaccurate reports, and that reports can be difficult for lay users to interpret correctly).

[39] Oyama, *supra* note 15, at 188–90.

[40] *Id.*

a criminal record, and once those assumptions are made they cannot be undone. In other words, the social stigmatization of the criminal status is so severe that subsequently learning a conviction was expunged usually does nothing to change the opinions of those people who had previously found out about the crime.[41] This means that as soon as employers or landlords discover that a person has a criminal record, the damage is likely irreparable.

Social stigmatization as a result of having a criminal record is a root cause for some of the collateral consequences associated with the commission of a crime. In that way, expungement can be thought of as a vehicle for alleviating at least some of those consequences.[42] *Black's Law Dictionary* defines "collateral consequences" as "[a] penalty for committing a crime, in addition to the penalties included in the criminal sentence."[43] Employers and landlords frequently rely on criminal background checks to vet applicants and often have policies in place that automatically disqualify an applicant based on his or her status as a convicted criminal.[44] Loss of employment or housing is likely the most common, and arguably most detrimental, collateral consequence ex-offenders face.[45] For this reason, the freedom from disclosing the existence of a criminal record, even when asked directly on an application, is traditionally thought to be a benefit of expungement. Take, for example, California's expungement law, which states:

> In any case in which a defendant has fulfilled the conditions of probation for the entire period of probation, or . . . in any other case in which a court, in its discretion and the *interests of justice*, determines that a defendant should be granted the relief available under this section . . . the court shall thereupon dismiss the accusations or information against the defendant and except as noted below, he or she *shall thereafter be released from all penalties and disabilities resulting from the offense* of which he or she has been convicted . . . .[46]

The phrase "released from all penalties and disabilities resulting from

---

[41] Geffen & Letze, *supra* note 27, at 1332.

[42] For a discussion of the expansive collateral consequences associated with criminal convictions, see Demleitner, *supra* note 32, *passim*.

[43] BLACK'S LAW DICTIONARY 298 (9th ed. 2009).

[44] Geffen & Letze, *supra* note 27, at 1340 (explaining that employers and landlords view criminal records as somehow being indicative of a tendency in the individual to be unreliable or dishonest and that such a presumption provides valid grounds for denying employment or housing in many if not most jurisdictions).

[45] Demleitner, *supra* note 32, at 156–57 (discussing the effects of ex-offender status on access to employment); Oyama, *supra* note 15, at 181 (describing the devastating effect of housing discrimination against those individuals with criminal records).

[46] CAL. PENAL CODE § 1203.4(a) (West 2004 & Supp. 2011) (emphasis added).

the offense"[47] is said to provide the source for this right of nondisclosure in California and has been interpreted by the California Court of Appeals to mean that persons granted relief under this statute are released from "the obligation to disclose the conviction in response to any direct question contained in any questionnaire or application."[48]

But wouldn't it also follow that in order for an expungement to be effective, information pertaining to the original conviction must be similarly unavailable through means *other* than disclosure by the ex-offender? As described below in Part III of this Comment, prior to the digitization of information, simply granting this freedom not to disclose—and serving the expungement order on the local or state agency maintaining records—was all that was needed to prevent the information from being unlawfully disclosed. However, in an internet era, simply granting individuals the freedom not to disclose the existence of their criminal record is no longer effective at preventing that information from being disclosed.

Expungement is a unique form of relief. It grants certain ex-offenders a "clean slate," essentially erasing the existence of a past offense.[49] In fact, in 1943, the Southern District of California, shortly after the passage of California's first expungement legislation, went so far as to equate expungement with the grant of a pardon, stating that:

> A pardon reaches both the punishment prescribed for the offence and the guilt of the offender; and when the pardon is full, it releases the punishment and blots out of existence the guilt, so that in the eye of the law the offender is as innocent as if he had never committed the offence. If granted before conviction, it prevents any of the penalties and disabilities consequent upon conviction from attaching; if granted after conviction, it removes the penalties and disabilities, and restores him to all his civil rights; it makes him, as it were, a new man, and gives him a new credit and capacity.[50]

If the intended result of an expungement is to render the offender "as innocent as if he had never committed the offence," then, carrying the reasoning of this court to its logical end, it is absolutely imperative that the existence of the offense itself be kept a secret after expungement.[51] In sum, expungement serves an important societal function in eliminating some of

---

[47] *Id.*

[48] People v. Mendez, 286 Cal. Rptr. 216, 219 (Cal. Ct. App. 1991).

[49] *Black's Law Dictionary* defines "expungement of record" as follows: "The removal of a conviction (esp. for a first offense) from a person's criminal record.—Also termed *expunction of record*; *erasure of record*." BLACK'S LAW DICTIONARY 662 (9th ed. 2009).

[50] *In re* Ringnalda, 48 F. Supp. 975, 977 (S.D. Cal. 1943) (quoting *Ex parte* Garland, 4 Wall. 333, 380–81 (1866)).

[51] Diehm, *supra* note 18, at 76 ("The expungement of a criminal record will be of little value if anyone acknowledges the record's existence.").

the collateral consequences associated with conviction and allowing individuals to reintegrate into society by obtaining employment and housing. Therefore, in order for expungements to continue to provide relief in an internet era, there must be a mechanism in place to ensure that post-expungement privacy violations do not occur.

III. THE DATA-BROKER INDUSTRY

The right to access public records, including court documents, is long established in the United States.[52] Accordingly, employers and landlords have long been able to obtain the criminal records of potential employees and tenants. However, it was not until after the advent of the internet in the early 1990s that America experienced an explosion of the data-broker industry.[53] Prior to that time, obtaining information from public records was very much a localized operation.[54] Generally, the person, company, or investigative agency for hire seeking information would obtain records on a case-by-case basis directly from whatever state or local agency maintained such records.[55] Essentially, prior to the invention of the internet and the creation of the private data-broker industry, the primary—if not singular—way of obtaining information about an individual's criminal record for the purpose of employment or housing was by obtaining information directly from a state agency.[56]

Now, however, we live in a different era. Consumer reports that contain criminal history are now widely available through the use of third-party private background check companies and oftentimes directly over the

---

[52] *See* Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978).

[53] SEARCH REPORT, *supra* note 10, at 29. According to a report from the Bureau of Justice Statistics, many scholars have also speculated that an increased demand for employee and tenant background checks after the events of September 11th has contributed to large industry growth. *See id.* at 31; James Jacobs & Tamara Crepet, *The Expanding Scope, Use, and Availability of Criminal Records*, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177, 204–05 (2007) (noting an increase in fingerprinting and background checks post-September 11th); Liptak, *supra* note 14 ("Since the attacks of Sept. 11, 2001, criminal background checks have become routine in many employment applications."); Oyama, *supra* note 15, at 187 ("Post-9/11 screening requirements have contributed to an 'explosion' in the demand for criminal background checks in employment and tenant placement.").

[54] David S. Ardia, *Reputations in a Networked World: Revisiting the Social Foundations of Defamation Law*, 45 HARV. C.R.-C.L. L. REV. 261, 310 (2010).

[55] *Id.* It's also worth noting that such records were usually maintained on paper and that obtaining a "copy" of records at that time meant that the person would receive a paper photocopy rather than digitized records, which are available now in many if not most jurisdictions.

[56] *Id.*

internet.[57] The process by which records are obtained and what types of records are available varies somewhat based on individual state laws.[58] However, modern data brokers, rather than obtaining information on a case-by-case basis, now purchase information in bulk from state and local sources and store that information in their own databases.[59] Over time these databases have grown substantially and the data contained therein often spans multiple jurisdictions and dates back many years.[60]

This Part will address two major issues that have contributed to the evolution of the modern data-broker industry. First, the demand for information at your fingertips has created strong industry incentives for data brokers to acquire massive databases and to grow them constantly, rather than update or eliminate old records. With the digitization of data and certain state and local practices making the accumulation of data more streamlined, these companies now have massive databases with information about private citizens. The second issue is that without regulation requiring these companies to update their records or punishing them for distributing false data, there are no disincentives to balance out the perverse incentives provided by the consumers. The result is a wildly unregulated behemoth of an industry that is quietly posing a threat to the privacy rights of American citizens.[61]

A. THE DATABASES: HOW INFORMATION IS COLLECTED, STORED, AND DUPLICATED

The general process by which the biggest data brokers obtain records is through what has been termed "bulk data purchases."[62] This entails the bulk purchase of criminal records for multiple individuals all at one time from state or local recordkeeping agencies and then storing that information in proprietary databases "for instant searches."[63] Early in the development of the data-broker industry, local agencies recognized the moneymaking potential in selling public records to data brokers, and many of those local

---

[57] SEARCH REPORT, *supra* note 10, at 7–9 (listing the key players in the data-broker industry); BEST BACKGROUND CHECKS, http://www.bestbackgroundchecks.com (last visited Nov. 11, 2011) (providing a directory of recommended data brokers in each state).

[58] SEARCH REPORT, *supra* note 10, at 39–43; *see, e.g.*, CAL. CIV. CODE §§ 1786–1786.2 (West 2009) (governing the process for obtaining and distributing public records in California).

[59] SEARCH REPORT, *supra* note 10, at 7–8, 10; Liptak, *supra* note 14.

[60] SEARCH REPORT, *supra* note 10, at 7–8.

[61] *See infra* Part III.B.

[62] SEARCH REPORT, *supra* note 10, 10–12.

[63] *Id.* at 10 (internal quotation marks omitted).

agencies now garner a considerable profit from the practice.[64] Notwithstanding limitations through some individual states' laws and practices,[65] local agencies are essentially free to give over public records to data brokers and turn a profit in the process.[66]

Furthermore, when the data-broker industry first blossomed, such databases were usually limited to one jurisdiction or at least single states; but over time data brokers began advertising national databases that would "allow users to almost instantly search proprietary databases containing upwards of 160 million criminal records from every State."[67] For example, one data broker's homepage boasts that "[w]ith one click [you can] search over 300 million criminal records drawn from the archives of US courts and correctional facilities."[68]

Essentially, once a large market emerged for private background checks,[69] those companies providing the most information the fastest gained a competitive advantage. In order to meet demand, these companies were incentivized to grow their own databases by accumulating records in bulk from state and local agencies rather than engaging in the time-consuming process of requesting records on an individual, case-by-case basis.[70]

---

[64] Oyama, *supra* note 15, 189 n.41 ("Some state and local governmental agencies have discovered the profitability in offering [to sell criminal records] at a price. For example, the Indianapolis Police Department makes criminal histories available at $15 per search on their website, http://www.civicnet.net/allservices.html; the South Carolina Law Enforcement Division charges $25 per name to perform a statewide criminal check on a name, http://www.sled.sc.gov/CATCHHome.aspx?MenuID=CATCH.").

[65] Some states have passed laws that limit or prohibit the sale of certain records—including criminal records—but these restrictions have actually had little effect on the data-broker industry as a whole. For an explanation and overview of these state regulations, see SEARCH REPORT, *supra* note 10, at 39–43. Some state agents simply refuse to engage in the practice of selling records precisely because of the potential for subsequent violations of post-expungement privacy. Liptak, *supra* note 14 (quoting a district clerk in Texas on the subject: "How the hell do I expunge anything . . . if I sell tapes and disks all over the country?").

[66] *See* SEARCH REPORT, *supra* note 10, at 39–43 (providing an overview of state statutes that regulate the sale and use of criminal records, but noting that very few are tailored to regulate data brokers).

[67] *Id.* at 11.

[68] *Criminal Records*, INFOREGISTRY, http://www.inforegistry.com/index.php?page=criminal_records (last visited Nov. 16, 2011).

[69] After the events of September 11, 2001, there was a sudden and significant rise in the demand for criminal background checks and consumer reporting services. *See supra* note 53.

[70] The growth of national databases began around 2001, suggesting that the demand for criminal records after September 11th created this industry incentive. *See* SEARCH REPORT, *supra* note 10, at 11 (stating that data brokers began accumulating nationwide databases in 2001); Oyama, *supra* note 15, at 187 (attributing the growth of the data-broker

Naturally, these companies have to provide accurate information or they would lose credibility with their customers. However, disclosing information from expunged records would not necessarily diminish their credibility, especially when considering data brokers' clientele. One can imagine that an employer or landlord who receives information from an expunged record might not be dissatisfied with the background check company at all; rather, the consumer would likely be pleased. Firstly, it is important to note that information about an expunged conviction is not *factually* incorrect.[71] The individual was found guilty of a crime in the past and granting an expungement does not make that fact any less true. Furthermore, it is highly likely that employers and landlords would be pleased to know that a potential employee or tenant *once* had a record, even if he or she did not anymore.

As discussed in Part II of this Comment, the stigma of a criminal record is incredibly strong. The suggestion being that the stigma associated with criminal status is so strong and so negative that landlords and employers will often deny housing and employment to individuals with criminal records based only on the fact of their having a record.[72] It is for this reason that data brokers face no industry pressure to avoid releasing information from expunged records. In fact, it is possible that because employers and landlords might respond positively to the disclosure of expunged records, data brokers actually have an incentive *not* to update records or perform due diligence before releasing information.[73] If state and local recordkeeping agencies no longer have that information, data brokers then become the only source from which employers and landlords could obtain information from expunged records—information that the data brokers' clientele would likely value.

The fact remains that the story of our hypothetical young man is not hyperbole.[74] Where criminal records were once contained in file cabinets at

---

industry to increased demand for criminal records after September 11th).

[71] For further discussion, see *infra* Part IV.A.

[72] *See supra* notes 44–45 and accompanying text.

[73] While there is no hard data to back up the argument that employers and landlords would appreciate the disclosure of expunged records, it is certainly not an unwarranted assumption based on the information cited in Part II of this Comment. Again, this is an area where empirical research is important to supplement efforts to reform the data-broker industry.

[74] Even though extensive data quantifying the issue is unavailable, there is evidence that background checks containing expunged records have had adverse consequences for individuals in the job and housing market. *See, e.g.*, Liptak, *supra* note 14 (discussing several cases where people were denied employment and housing based on the disclosure of their expunged records by background check companies). One man was denied employment

local courthouses and halls of records, they are now mobile, capable of rapid duplication, and readily accessible in electronic form.[75] They are being stored in massive, privately maintained databases and they are rarely, if ever, updated.[76] Finally, the combination of the industry's incentive not to update and increased access to information through the growth of the industry creates an alarming likelihood that incorrect or harmful information will come to light.[77] Although it is unclear how frequently outdated or expunged records are released, industry practice suggests it is likely happening with alarming frequency.[78]

B. AN UNREGULATED INDUSTRY

Not only is there an industry incentive *not* to update records, but there is also no counterweight to that incentive. As it stands, data brokers are not required to exercise any due diligence with respect to the release of

---

based on the disclosure of his expunged record and is now suing both his potential employer and the data broker that provided the information. An unidentified woman was unable to purchase a condominium because her expunged conviction appeared on a background check. And a third, unidentified man was unable to procure employment for six months due to an expunged conviction appearing on his background check. *Id.*

[75] SEARCH REPORT, *supra* note 10, at 10 (discussing the increasing digitization of court records); Oyama, *supra* note 15, at 187 ("By 2003, 94% of the criminal history records maintained by the state criminal history repositories were automated (71 million records).").

[76] SEARCH REPORT, *supra* note 10, at 11–12 ("Updates are typically available on a monthly basis. This varies, however, depending not only upon how often the sources make updates available, but also on whether the vendor promptly obtains the update and integrates it into existing products. Updates may include only new records or they may also include updated or deleted records. As a result, vendors customarily prefer to obtain an entirely new copy of the database because this relieves the vendor of having to merge a small subset of updates into an existing system . . . . [T]he commercial vendor must be proactive, submitting orders and payments to the court or agency, which subsequently sends the data."). As noted above, there is no incentive for vendors to incur the extra cost or exert the extra effort in obtaining updates in this way.

[77] Once again, no empirical studies have been conducted to determine the number of people who have been, or might be, adversely affected by the release of expunged records. This is possibly due to the fact that employers and landlords do not always disclose their reasons for denying employment and housing. *See* Jacobs & Crepet, *supra* note 53, at 212 ("Employers may actually disqualify job applicants based on a criminal record, but offer other reasons or no reason at all for having rejected the ex-offender in favor of another job applicant."). Or perhaps it would be very difficult to determine how many criminal records that have since been expunged are still being stored in private databases. Ultimately, such a study would be an interesting, if not vital, follow-up to this argument.

[78] As this Section argues, the industry provides disincentives for data brokers to be proactive in seeking out updated records, and Part III.B of this Comment discusses the lack of regulation that would compel them to do the same. The resulting combination of factors strongly supports an inference that expunged records are stored in private databases and released without consequence.

expunged records.[79] This Section addresses the current process for removing information from propriety databases and how that process—individual enforcement—is inadequate to protect post-expungement privacy. Next, this Section discusses the Fair Credit Reporting Act (FCRA), which is the only federal statute even tangentially related to data brokers. However, this Section will show that the FCRA's provisions were not designed to regulate data brokers, making it an inefficient vehicle for protecting post-expungement privacy. Finally, this Section concludes by proposing a need for an independent statutory system specifically designed to regulate the data-broker industry.

Currently, the only way to remove an expunged conviction from a data broker's records is to personally request that the information be removed. This process is arduous and involves the submission of several documents including court dispositions and expungement orders.[80] In fact, some data brokers even require that one submit along with this request a copy of the information as it appears on the report from their websites.[81] This requirement is particularly troubling because it forces individuals to purchase their own consumer reports before finding out whether any one database contains an expunged conviction.

Even with a system that would *easily* allow an individual to remove

---

[79] SEARCH REPORT, *supra* note 10, at 11–12 (discussing the lack of regulation requiring data brokers to update their records and noting that updates are scarcely available for even those data brokers that might want to update their records).

[80] *See, e.g.*, Email from Lucy, Customer Serv. Representative, InfoRegistry.com, to [name redacted] (Nov. 22, 2010) (on file with author) (responding to an inquiry into the process for removing information from expunged records). This email responded as follows:

> The best way to ensure that your information is removed properly is to contact us. As a courtesy, you may opt-out of having certain of your information included in the Data that appears in search results if one of these conditions exist: (1) You are a state, local or federal law enforcement officer or public official and your position exposes you to a threat of death or serious bodily harm; or (2) you are a victim of identity theft; or (3) you are at risk of physical harm; or (4) you have evidence the record is incorrect or expunged. To opt-out, submit the following information: 1) A written explanation for the opt out request. Identify the specific location of Your Data on our Website, and where your personal Data is publicly available, identify one of the four conditions You [sic] enabling you to opt-out of having your personal Data removed, and describe why such personal Data that is publicly available is inaccurate and harmful. NOTE: Please submit ONE request per individual. 2) Copy of your current driver's license or state identification (this information is necessary in order for us to authenticate that the request is being made by the individual to whom the information belongs to). All requests must include: [f]ull name and date of birth, [a]liases, if any, [c]urrent address, [p]revious addresses, [p]hone, [e]mail address. 3) Specific complete details of the records you are requesting to be removed. NOTE: Only your current and up to two previous address records will be removed. 4) Include a print out of the records you wish to have suppressed. 5) Copies of any applicable court orders, if any.

[81] *Id.*

his or her own information, individual enforcement is still ineffective at fixing the problem for more than just that one individual.[82] As discussed above, by the time that most individuals are made aware of the information in these databases,[83] the information has likely already been released and the individuals have already suffered the negative consequences.

The only mechanism that currently regulates the activities of credit and background check companies is the FCRA.[84] However, there are several issues that prevent the FCRA from being a successful tool in addressing the specific issues associated with data brokers and post-expungement privacy. Primarily, the FCRA does not impose any affirmative duties on data brokers to update their records, and its enforcement provisions still put the onus of ensuring compliance on individual persons. In sum, the FCRA is impotent to address the problem at issue and may even help to contribute to post-expungement privacy violations rather than curb them.[85]

When the FCRA was drafted in 1970, the internet as we have come to know it had not yet been invented[86] and any consumer information or public records were still largely kept on paper. The result was a piece of legislation that failed to comprehend the ease with which information would one day be collected and widely disseminated.[87] After all, how could the members of Congress in 1970 anticipate the information age?

However, even with its current amendments, the FCRA still does not

---

[82] Furthermore, even if a person succeeds at removing the information from one broker's proprietary database, the person would likely have to repeat the process for every other broker that could potentially have purchased his records. Oftentimes, multiple data-broker companies maintain separate databases. Thus, each individual with an expunged record would have to contact each data broker and go through its arduous process to request that the information be removed.

[83] That is, if they are ever even made aware. *See supra* notes 43–44, 77 and accompanying text.

[84] Fair Credit Reporting Act (FCRA), 15 U.S.C § 1681 (2010). The FCRA applies, in part, to any "consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, . . . [p]ublic record information." *Id.* § 1681a(p).

[85] For an enlightening discussion of the FCRA and its flaws, see De Armond, *supra* note 38, at 1098–1118.

[86] *See generally The Internet: A Short History of Getting Connected*, FED. COMM. COMMISSION, http://www.fcc.gov/omd/history/internet/ (last visited Oct. 30, 2011).

[87] It also bears mentioning that many state expungement statutes were also drafted prior to the information era and so likely also failed to anticipate the digitization of data. *See, e.g.*, Act of July 15, 1935, ch. 604, § 5, 1935 Cal. Stats. 1709–10 (codified as amended at CAL. PENAL CODE § 1203.4 (West 2008 & Supp. 2011)); Sentencing Reform Act of 1981, ch. 137, § 23, 1981 Wash. Sess. Laws 531 (codified as amended at WASH. REV. CODE ANN. § 9.94A.640 (West 2010)); *see generally* Liptak, *supra* note 14.

necessarily apply to all private data brokers selling criminal records to private citizens.[88] The FCRA was created with the aim of ensuring that "consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[89] In 1998, the Federal Trade Commission issued an advisory letter confirming certain sections of the FCRA applied to agencies that provide criminal records information for employment purposes.[90] But many data brokers still escape regulation and liability under the statute.[91] This is likely because the general spirit of the FCRA—especially evident in its citizen-suit provision[92]—is to protect consumers with respect to financial and other consumer credit data, not with respect to criminal records.[93] One such provision that evinces the legislature's intent to move away from

[88] The FCRA defines a consumer reporting agency and what activities are covered under its provisions. *See supra* note 95. However, these provisions are written is such a way that data brokers are able to define themselves out of the FCRA's grasp. *See, e.g.*, Email from Lucy, *supra* note 80 ("Please be aware that we are not a 'consumer reporting agency' as defined by the FCRA, as we do not provide any data for use in credit, insurance, or employment screening. We explicitly prohibit the use of our service and the data it supplies for such purposes.").

[89] FCRA § 1681(b).

[90] Advisory Letter from William Haynes, Division of Credit Practices, Fed. Trade Comm'n, to Richard LeBlanc, Due Diligence, Inc. (June 9, 1998), *available at* http://www.ftc.gov/os/statutes/fcra/leblanc.shtm (regarding Sections 603, 607, and 609 of the Fair Credit Reporting Act).

[91] *See supra* note 88.

[92] It is worth noting that as of July 26, 2011, certain sections of the citizen-suit provision of the FCRA were rescinded. Statement of General Policy or Interpretation; Commentary on the Fair Credit Reporting Act, 76 Fed. Reg. 44462-01 (July 26, 2011) (rescinding 16 C.F.R. §§ 600.1–.2). However, because these changes are so recent, it is unclear what their effect will be on future litigation against data brokers under the FCRA. These changes may reflect an effort to bring data brokers under the fold of the FCRA, but it is also possible that they will push data brokers further out of the FCRA's grasp as some past amendments have done. *See infra* note 93. Regardless of the potential effect of these changes to the FCRA, the purpose of this Section is to illustrate how the FCRA has not yet been successful at regulating data brokers. Therefore, this Section includes cases and articles analyzing the FCRA prior to the recent rescission.

[93] The 2003 amendments removed a provision prohibiting the release of criminal convictions dating back more than seven years, thus allowing credit reporting agencies to hold on to criminal records indefinitely. Fair and Accurate Credit Transactions Act of 2003 (FACTA), Pub. L. No. 108-159, 117 Stat. 1952 (2003); *see also* Geffen & Letze, *supra* note 27, at 1339. While it is possible that this provision was removed in order to preserve the statute's purpose as being confined to consumer-credit agencies, it is certainly true that by removing protections on criminal records, the FCRA became less effective at regulating the data-broker industry.

regulating data brokers is the fact that the FCRA allows criminal convictions to be reported indefinitely.[94] This provision *encourages* the disclosure of expunged records rather than serving to regulate the practice.

Furthermore, even if the FCRA applied to all data brokers, the only restriction that it would place on them is the requirement that they "follow reasonable procedures to assure maximum possible accuracy."[95] This vague and ambiguous standard hardly imposes an affirmative duty upon data brokers to update their records. In fact, courts have interpreted this accuracy provision as requiring data brokers only to "weigh the potential that the information will create a misleading impression against the availability of more accurate [or complete] information and the burden of providing such information."[96] Essentially, the FCRA allows data brokers to pass on unvetted information without suffering any consequences, even if the information turns out to be incorrect.[97]

This leads to the second reason why the FCRA does not adequately regulate problems specifically associated with post-expungement privacy. Not only does the FCRA fail at imposing affirmative duties on data brokers, its enforcement provisions are both textually and practically insufficient to provide consumers with a remedy *after* their post-expungement rights have been violated.[98] The FCRA contains a citizen-suit provision that allows civil causes of action for both willful and negligent noncompliance with the FCRA provisions.[99] However, as discussed above, courts have interpreted the responsibilities of data brokers under the FCRA's accuracy provisions to be so minimal that plaintiffs rarely prevail in such suits.[100] The result is a statutory scheme that fails to regulate the release of harmful, false information and then fails to provide an adequate remedy for those who are directly harmed when the information is released.

---

[94] *See* Geffen & Letze, *supra* note 27, at 1339.

[95] FCRA § 1681e(b); *see also* Haynes, *supra* note 90.

[96] *See, e.g.*, Koropoulos v. Credit Bureau, Inc., 734 F.2d 37, 42 (7th Cir. 1984).

[97] De Armond, *supra* note 85, at 1102–03; *see, e.g.*, Smith v. Auto Mashers, Inc., 85 F. Supp. 2d 638, 641 (W.D. Va. 2000) (dismissing a complaint against a data broker on the grounds that "simply by reporting an item of information that turns out to be inaccurate" is not a violation of the FCRA).

[98] Notwithstanding the fact that ex post remedies fail to prevent or remedy harms associated with post-expungement privacy, this Section will discuss the inadequacies of the FCRA in providing *any* sort of remedy for those individuals whose post-expungement rights have been violated. See *infra* Parts IV–V for a discussion dismissing ex post remedies in the post-expungement privacy context.

[99] FCRA § 1681n (imposing civil liability for willful noncompliance), *id.* § 1681o (civil liability for negligent noncompliance).

[100] De Armond, *supra* note 38, at 1103–04.

The FCRA is the only statute that currently governs the data-broker industry, and it is woefully inadequate to address the issues of post-expungement privacy. Therefore, a comprehensive legislative mechanism specifically designed to regulate the data-broker industry is needed to protect post-expungement privacy rights.

IV. SUPPORT FOR A FEDERAL STATUTE

This Part will argue that a federal statute is the only remedy likely to have a significant effect on the violation of post-expungement privacy rights. This Part first explores and dismisses individual, private common law causes of action as one possible remedy.[101] Next, this Part addresses the possibility of state regulation, but ultimately dismisses this as ineffective due to the national reach of the data-broker industry. Finally, this Part discusses the authority under which a federal statute can be devised and will make arguments for such a statute's comparative superiority to the other two remedies aforementioned.

A. WHY PRIVATE CIVIL CAUSES OF ACTION ARE INADEQUATE

An individual private right of action is one possible way to enforce post-expungement privacy laws. One type of private civil action—action under the FCRA—has already been discussed and dismissed as an inadequate remedy in Part III of this Comment. However, there are other civil actions that would provide possible methods for enforcing post-expungement privacy rights. This Comment ultimately argues that such individual remedies without the support of a larger government regulatory scheme would be inadequate to address the scope of this issue. The overarching and most salient reason is that there is essentially no way to provide any ex post remedy when post-expungement privacy rights have been violated; no one can un-ring the bell. However, there are also problems with individual civil remedies—such as the tort of defamation—in that those traditional causes of action would not support claims for violations of post-expungement privacy even if such claims would be valuable to potential plaintiffs.

In January 2011, the New Jersey Supreme Court decided *G.D. v. Kenny*.[102] This case involves a defamation[103] suit based on the disclosure of

---

[101] This Comment uses the example of defamation suits in representing all private common law causes of action.

[102] 15 A.3d 300 (N.J. Sup. Ct. 2011).

[103] In New Jersey, defamation is a tort that is defined as follows: "In order to prove defamation, a plaintiff must establish, in addition to damages, that the defendant (1) made a defamatory statement of fact (2) concerning the plaintiff (3) which was false, and (4) which

information from expunged criminal records. The facts of the *G.D.* case were as follows: the plaintiff, a former aide to a political candidate in New Jersey, brought a defamation claim against members of an opposing candidate's staff who had circulated political smear fliers referring to the plaintiff's drug-related convictions, which had previously been expunged.[104] The plaintiff claimed that the fliers constituted defamation (as well as several other torts) and the defendant claimed truth as a defense.[105] The New Jersey Supreme Court ultimately decided for the defendant on three separate grounds: first, that the defendants were entitled to a truth defense;[106] second, that the fliers were substantially true;[107] and third, that the plaintiff did not have a reasonable expectation of privacy just because his convictions were expunged.[108]

This case is particularly pertinent for several reasons. The court's three holdings highlight two different problems with defamation suits for post-expungement privacy violations. First, the problem of truth:[109] in allowing defamation suits for the disclosure of expunged convictions, courts would be creating a legal fiction whereby the fact of a conviction somehow becomes "untrue" once it has been expunged. One could argue—as G.D. did[110]—that the statements have a defamatory nature because the

---

was communicated to a person or persons other than the plaintiff." Feggans v. Billington, 677 A.2d 771, 775 (N.J. Super. Ct. App. Div. 1996) (citing Bainhauer v. Manoukian, 520 A.2d 1154 (N.J. App. Div. 1987)).

[104] *G.D.*, 15 A.3d at 306. The flier, including a picture of the plaintiff, read:

> TEAM STACK: COKE DEALERS. GUN RUNNERS. EX-CONS[.] THE MORE PEOPLE KNOW, THE MORE QUESTIONS THEY HAVE ABOUT BRIAN STACK. UNION CITY MAYOR BRIAN STACK'S CLOSEST POLITICAL OPERATIVES: GUN RUNNERS, COKE DEALERS, EX-CONS. We all know the threat that drugs and illegal guns have in our communities. But not Brian Stack. He continues to surround himself with one shady character after another—not one but two convicted drug dealers and ex-cons, whom Stack got a high paying county job and a drugged out gun running lowlife who was his campaign manager. BRIAN STACK PREACHES "REFORM" AND "GOOD GOVERNMENT" BUT HIS ADMINISTRATION IS MADE UP OF SLEAZY DRUG DEALERS AND OTHERS WHO SHOULD BE NOWHERE NEAR THE PUBLIC TREASURY.

Id. (line breaks omitted).

[105] *Id.* at 304.

[106] *Id.*

[107] *Id.* ("Although our expungement statute relieves a prior offender of some civil disabilities, it does not extinguish the truth.").

[108] *Id.*

[109] This problem encompasses the court's first two holdings that the defendants are entitled to a truth defense and that the fliers were substantially true.

[110] *G.D.*, 15 A.3d at 307–09.

expungement itself renders them essentially untrue.[111] However, the fact remains that the conviction did occur and just because it was expunged does not make it untrue.[112] As the New Jersey Supreme Court noted, truth is not just a common law defense to defamation but it is also protected by the First Amendment.[113] From the perspective of a defendant in a defamation suit for post-expungement privacy violations, a finding of liability would erode those First Amendment rights. And for what? The most any plaintiff can hope for is monetary damages because the harm caused by the release of information cannot be undone.

To further prove the point, consider a situation where the alleged defamer also discloses that the record was expunged. This statement would still harm the defendant in the same way—because it discloses the existence of their criminal record—but, in this instance, it is a completely true statement because the defamer also discloses that the record was expunged. The fact remains that the release of expunged records can cause the same type of harm that ordinary defamatory statements can. However, the fact of expungement does not render those statements untrue, and thus post-expungement privacy claims do not fit squarely into the tort of defamation.[114]

The final part of the *G.D.* court's holding, that G.D. did not have a reasonable expectation of privacy, highlights another complication with civil suits as a remedy for post-expungement privacy violations—the fact that convictions are made public. The New Jersey Supreme Court noted that arrests, indictments, and convictions are a matter of public record,[115] and as a result newspapers, magazines, court reporters, individuals, and

---

[111] As discussed in Part II of this Comment, expungements grant citizens the right to proceed as if they were never convicted of a crime and to be free of the "criminal" designation. Following that logic, one could argue that disclosing the fact of an expunged criminal conviction is untrue because that person is no longer a "criminal." This is the spirit of what G.D. attempts to argue. *Id.* at 307–09.

[112] The New Jersey Supreme Court belabors this point several times throughout its opinion. *See, e.g.*, *id.* at 304, 310, 313.

[113] *Id.* at 310 ("The law of defamation attempts to strike the proper balance between protecting reputation and protecting free speech." (quoting Ward v. Zelikovsky, 643 A.2d 972, 978 (N.J. 1994) (internal quotation marks omitted)).

[114] It is possible that courts in other jurisdictions may decide this issue differently than the court in *G.D.* did. However, even if post-expungement privacy violations could form the basis of a defamation (or other tort) suit, such suits would still be ineffective at addressing the root of the problem: that expungement itself is ineffective unless post-expungement privacy violations can be prevented. And post-expungement privacy violations can never be prevented with ex post remedies, like those available in civil suits.

[115] *G.D.*, 15 A.3d at 309.

even data brokers lawfully obtain that information.[116] It is true that when a conviction is expunged, the information is no longer available to the general public through *official* channels, but it is still legally available from any of those other sources.[117] The *G.D.* court deftly observes that "[a]ll of the beneficial purposes of the expungement statute, and the protections it provides, will not allow a person to fully escape from his past."[118] In other words, because information from expunged records is readily available, and it is currently legal for non-government sources to maintain and provide that information, the current common law system will never support individual civil actions for post-expungement privacy violations.

In conclusion, post-expungement privacy violations are uniquely unsuited for civil tort suits, both because the information from those records is not untrue and because civil suits would have little effect on the overarching problem of post-expungement privacy violations. Without being incorporated into a larger statutory scheme, such suits merely place small bandages on a gaping wound. As the New Jersey Supreme Court made clear in its observations, the data-broker industry has already grown to epic proportions and is proceeding unregulated, so the problem is far too big to resolve without going to the source and regulating the companies themselves.

B. WHY STATE STATUTES ARE INADEQUATE

State regulations are another possible solution to regulate violations of post-expungement privacy by data brokers. In an ideal world, if every state simultaneously enacted legislation, this could be a potential solution; but because data brokers maintain and distribute records throughout the nation, this solution is inadequate.

Some states have already recognized this problem and attempted to address it through regulation of employers and landlords rather than data brokers.[119] Some state regulations, along with some helpful federal provisions of Title VII,[120] prohibit the use of expunged criminal records to discriminate against applicants when making employment and housing

---

[116] *Id.* at 312–13.

[117] *Id.* at 313.

[118] *Id.*

[119] SEARCH REPORT, *supra* note 10, at 61–65 (describing the various state laws that govern the use of criminal convictions and arrests in making housing and employment decisions).

[120] *Id.* (comparing Title VII's provisions governing the use of criminal records to those of individual state statutes, the states' statutes being more robust).

decisions.[121] Other state statutes regulate the dissemination of information.[122] Currently, the only type of state law that directly regulates data brokers is laws controlling the dissemination of government information to data brokers. However, even if individual states aggressively regulated the dissemination of data, at this point in time, it is too little too late.[123] Since data brokers have already amassed significant databases over time, they currently possess millions of records, some of which have either already been expunged or might be expunged in the future. Thus, stopping the flow of records to these databases now would do nothing to prevent the release of records that they already have.

Because employers and landlords are more easily reached through state police powers than are national data brokers, the current state regulations make sense from the states' perspective. However, such regulation is ineffective for two main reasons. First, in the contexts of at-will employment and housing, employers and landlords have nearly free rein to choose one applicant over another. Thus, a law prohibiting discrimination on the basis of an expunged record would just encourage these employers to find a pretextual reason to discriminate against ex-offender applicants. After all, "when choosing between an ex-con and a person without a criminal past, most employers are likely to choose the latter."[124] Second, these regulations do not address the ultimate issue—they do not prevent data brokers from releasing expunged records. It is this preventative goal that is most important and needs to be addressed if there is any hope of protecting post-expungement privacy.

An important consideration in dismissing state regulation and proposing a federal statutory scheme is whether such a scheme might

---

[121] *See id.*; Geffen & Letze, *supra* note 27, at 1348 n.86 and accompanying text.

[122] SEARCH REPORT, *supra* note 10, at 26–27 ("State law largely regulates noncriminal justice access to information in the State repositories. Repositories in 43 states and territories responded to a March 2001 SEARCH email survey regarding the extent to which they disclose criminal history information to the public (that is, to noncriminal justice users such as employers and vendors). More than two-thirds of the responding repositories reported disclosing at least some criminal history information to the public. Information disclosed by the State repositories varies widely, depending upon State law. Some States disclose everything on file, with the exception of sealed or expunged records, while others disclose only adult offender conviction data that is less than 10 years old. Some States require the submission of the subject's fingerprints as a prerequisite for disclosure, while others make information available on the basis of name-plus-identifier checks." (footnote omitted)).

[123] However, the federal statute that this Comment proposes should contain provisions regulating the dissemination of information.

[124] Hacker, *supra* note 32, at 471 (footnote omitted).

infringe on state sovereignty.[125] Any time a federal regulatory scheme is proposed in an area that is traditionally reserved for the states, federalism concerns are inevitably going to surface. However, in this circumstance, even though regulating expungement and the maintenance of criminal records is typically reserved to the states, there is a strong argument to be made that regulating the data-broker industry is a separate issue capable of federal regulation under Commerce Clause authority.[126]

C. WHY A FEDERAL STATUTE IS SUPERIOR

First, Congress has the power to regulate both the channels of commerce and all things that are in, of, or about interstate commerce.[127] There is no doubt that the sale and purchase of criminal records across state lines is a part of interstate commerce. Similarly, the data brokers themselves are, in a sense, vehicles for interstate commerce. Finally, and in a much more tangential sense, the fact that the sale and purchase of records *for the purpose of employment and housing* has an effect on the job and housing markets could be found under the aggregating effects test[128] to also give Congress the authority to regulate in this area. Furthermore, the FCRA—at least with respect to sovereignty concerns—is already regulating a very similar market and paves the way for the type of regulation that this Comment proposes.[129] In sum, it is clear that Congress has the power to regulate the data-broker industry through the Commerce Clause.

With that in mind, a federal regulatory scheme is the best solution for

---

[125] The following is only a brief discussion of federalism concerns as they apply to the creation of a federal statute, and this Comment does not purport to present a full analysis of the issue.

[126] *See infra* Part IV.C.

[127] Original authority for commerce power is derived from Article I, Section Eight, Clause Three of the United States Constitution, which provides *inter alia* that Congress shall have the power to "regulate Commerce with foreign Nations, and among the several States." U.S. CONST. art. I, § 8, cl. 3. However, that power has been interpreted by the judiciary to include the power to regulate the channels of interstate commerce, all things that fall within interstate commerce, and those things that substantially affect interstate commerce. *See, e.g.*, Nat'l Labor Relations Bd. v. Jones & Laughlin Steel Corp., 301 U.S. 1 (1938); Champion v. Ames, 188 U.S. 321 (1903) (in, of, and about interstate commerce); Gibbons v. Ogden, 22 U.S. 1 (1824) (channels of interstate commerce). For a discussion of the history and evolution of Congress's commerce power, see Jack M. Balkin, *Commerce*, 109 MICH. L. REV. 1 (2010).

[128] *See Nat'l Labor Relations Bd.*, 301 U.S. 1 (first iterations of aggregation); Gonzales v. Raich, 541 U.S. 1 (2005) (modern aggregation).

[129] In fact, it has been proposed by some that effective regulation of the data-broker industry could even be accomplished through amendments to the FCRA itself. *See* SEARCH REPORT, *supra* note 10, at 71–72 (analyzing whether the FCRA should be amended to reach data brokers).

protecting post-expungement privacy rights. Such a scheme is preferable to individual private rights of action.[130] This is because citizen suits fail to effectively address large-scale post-expungement privacy violations. Furthermore, an ex post remedy fails to regulate the data-broker industry as a whole and thus does nothing to *prevent* violations from occurring in the first place. Although state statutes have some potential to regulate data brokers, on a larger level they will remain ineffective because these companies operate nationally and state laws cannot get to the "heart of the monster," so to speak. However, a federal statutory scheme should still pave the way for individual state regulation to come in and fill in the pieces, for example with regulations that limit the dissemination of information in the future.

In sum, federal legislation is the most effective way to address post-expungement privacy because the problem is simply too large. Data brokers' proprietary databases now span multiple jurisdictions and date back many years.[131] The data-broker industry has already been allowed to go on too long threatening the privacy rights of American citizens. Accordingly, the only effective way to curb continuing violations is through regulation that would apply universally to all data brokers and to all of the information in their databases.

V. PROPOSED AIMS FOR FEDERAL REGULATION

The final Part of this Comment provides proposed aims and suggested provisions for a federal statute designed to protect post-expungement rights. This Part considers first provisions designed to place an affirmative duty on data brokers themselves, then provisions designed to regulate state and local agencies, and finally provisions relating to enforcement.

A. AFFIRMATIVE DUTIES FOR DATA BROKERS

The first provision of the statute must define which companies fall within the regulatory scheme. The statute must cover any company that profits from the sale of information from public records, including arrests and convictions. The danger with respect to defining the scope of the statute is to ensure that all data brokers, as discussed and defined herein, are subject to restriction, without including media sources or other private sources of information.[132]

---

[130] However, a citizen-suit provision should still be included within the federal regulatory scheme. *See infra* Part V.

[131] *See supra* Part II.

[132] Specifically, the statute must be careful not to implicate newspaper archives or other

Once the statute defines which agencies are subject to its provisions, the statute must also clearly state that it is limited to expungement of misdemeanors and arrests that do not result in conviction.[133] The reasons are similar to this Comment's purpose in excluding them from its discussion: that policy debates and variations in state laws with respect to felony, juvenile, and sex-related convictions would complicate federal regulation. Also, because of these variations between state laws, it might be inappropriate for federal regulation to step in where some states may have chosen not to regulate. Finally, once the statute has limited the scope of its application, it must include provisions that impose affirmative duties directly on data brokers.

1. Prohibition on Willful or Negligent Disclosure

One provision of the statute must place an affirmative duty on data brokers to refrain from either willfully or negligently disclosing incorrect information, including the disclosure of convictions that have been expunged. However, the standard for negligent disclosure must be much more stringent than those found in the FCRA. Under the FCRA, companies distributing information must only "maintain 'reasonable' procedures to assure maximum possible accuracy."[134] As discussed in Part III.B, this places an extremely light burden on credit-reporting agencies.[135] The burden is so light that they are rarely, if ever, found liable for violations of the aforementioned provision.[136] The provision proposed here should require that data brokers exercise reasonable care in ensuring that the information they are distributing is correct. The reasonable care standard would be met by performing the regular updates in accordance with Part V.A.2 below. Furthermore, should incorrect information or information from expunged records be released due to a failure in updating, a company would be considered negligent per se and subject to sanctions as per Part V.C below.

---

websites and publications that, while they may profit from the release of information pertaining to criminal records—by the sale of their papers—are not agencies that intentionally maintain and distribute criminal records themselves for profit. Essentially, this statute should be limited so as not to require those media sources that report on public trials to be held liable for making archives of their past editions available to the public.

[133] *See supra* Part II.

[134] FCRA, 15 U.S.C § 1681e(b) (2010).

[135] *See supra* Part III.B.

[136] *See supra* notes 96–97 and accompanying text.

2. Regular Updates

Next, there must be a provision requiring that brokers regularly update their records. How often these companies should be required to update their records would have to depend on a survey of state and local record-keeping agencies to ascertain how frequently updates can be made available. However, once every six to eight months would be ideal, as expungements are granted regularly.

3. Disposing of Records

The next provision should require that data brokers dispose of records of criminal convictions and arrests after a certain number of years have elapsed, perhaps borrowing the seven-year time period that was once included in the FCRA. The policy justification is to curb the proprietary databases and to provide an additional incentive for data brokers to seek out updates. One suggestion would be to perform a multi-state survey of the average number of years that it takes to expunge different offenses and then limit data brokers accordingly. Regardless, this provision should also be retroactive in that it applies to all records that, at the time the statute is passed, date back longer than the statutorily prescribed maximum period. This retroactivity provision would be incredibly useful in purging the already existing databases that pose a potential threat to post-expungement privacy in the future.

4. Standardization of Reporting

The statute must also set guidelines for the standardization of reporting information from criminal records. Because of variations in the way different jurisdictions report and maintain their records and differences in local laws, data brokers often "normalize" information using their own internal system.[137] This can result in misinterpretation and subsequent misinformation when the final consumer report is produced.[138] Such practices can have harmful effects even for those individuals whose criminal records have not been expunged. For example, a consumer report could say nothing more than "drug-related conviction," which could refer to a large range of possible charges from possession to sale and including everything in between. Such potential for confusion and misinformation in the current system must be remedied. Again, the best system for normalizing these reports should be developed through comparison of current state and local reporting systems. But with the limited scope of this

---

[137] *See supra* Part III.

[138] *See id*.

statute, it should not be too difficult to normalize reporting.

B. REGULATING STATE AND LOCAL AGENCIES

It is also vital that any proposed statutory scheme put some limitations on the dissemination of data by state and local agencies. While such a provision might pose some federalism issues, in order to curb the privacy violations caused by the data-broker industry, it is important that data brokers no longer have the unfettered access to criminal records that they have now.

In order to require that data brokers regularly update their records, any state agency providing criminal records should have a concurrent duty to regularly update records and provide such updates to data brokers. While directly regulating the practices of state agencies would likely be outside of the Commerce Clause authority,[139] Congress could attach the requirement of regular updating as a condition on selling records in interstate commerce. Provided that Congress could attach such a condition, possible ways in which updates would be available should be determined by, again, surveying state and local practices to determine the best possible procedure. One suggestion would be for state and local agencies to send updates along with invoices as a condition upon the sale of records to data brokers—which some states are already in the practice of doing.[140]

C. ENFORCEMENT

Finally, and perhaps most importantly, this Comment proposes a set of comprehensive enforcement provisions that put the onus of responsibility on the data brokers. These enforcement provisions are necessary to create the most effective statute possible.

1. Monetary Sanctions

The statute must include a provision providing monetary sanctions that attach to any data broker who violates any provision of the statute. For example, any data broker that releases inaccurate information, including information about an expunged conviction, will face a fine. The amount should be appropriate to sufficiently deter data brokers from the practice

---

[139] Such regulation would also implicate concerns associated with compelling states to take certain actions under Commerce Clause power. *See* New York v. United States, 505 U.S. 144 (1992) (holding that the so-called take-title provision of a federal statute was unconstitutional essentially because it amounted to Congress compelling a state to comply with federal regulations).

[140] SEARCH REPORT, *supra* note 10, at 11.

and incentivize due diligence. Furthermore, liability under this section should be on a strict liability basis as opposed to by the level of culpability of the data broker. The reason for a strict liability standard with respect to monetary sanction is so that whatever administrative agency—likely the FTC—is in charge of enforcement will not have to hold hearings to determine culpability each time a data broker releases incorrect information. Naturally, the dollar amount per infraction would be adjusted down to account for a strict liability standard. Lastly, monetary sanctions should also attach, and at a higher amount, for failure to update regularly as per the updating procedures recommended herein.

2. Civil Sanctions

The statute should also provide civil sanctions for violation of its provisions. One possibility might be revoking or suspending the business licenses of those companies that fail to comply with the statutory provisions. Another might be something like an audit, where companies consistently in violation would be subject to more stringent review. Regardless of what particular sanctions should be in place, having civil sanctions on top of monetary penalties would necessarily strengthen the enforceability of the statute.

3. Citizen Suits

Lastly, it is imperative that the statute contains a citizen suit provision that both provides a means for reporting violations of the statute to the appropriate administrative agency and allows for private rights of action for harm caused by such violations. Citizens whose rights have been violated are without a doubt the most effective policing tools in this type of statutory scheme, and so the statute must provide a venue for such citizens to report violations to the appropriate administrative body. The statute should also provide for injunctive relief to prevent the release of incorrect information before that information causes harm. This provision would also require that data brokers honor expungement orders, and this portion of the statute should outline standardized procedures for private citizens to request their information be removed from proprietary databases. Finally, citizens who have been harmed by the release of incorrect information should have a clear cause of action for compensatory and punitive damages in civil court.

VI. CONCLUSION

This Comment has identified a largely unregulated industry that poses a threat to the privacy rights of individual citizens. Accordingly, the goal of this Comment is twofold: first, to clearly identify the issue and pave the

way for the kind of empirical study that is needed to move this issue into Congress's cognizance; and second, to propose a solution that would help protect individuals with expunged records.

We know that data brokers have amassed significant databases of criminal records, spanning many years and across many jurisdictions. We know that they are not currently required to update their records and—at least with respect to records that have been expunged—are incentivized not to seek out updates from state agencies. We know that expungements are granted every year in all of the states that have expungement statutes. We know that the release of expunged records has had a negative effect on at least some American citizens. We cannot ignore the possibility that data brokers are posing a significant threat to post-expungement privacy. The problem of unauthorized or unlawful release of expunged criminal records by data brokers can be devastating to the lives of people with expunged records. Something must be done to protect against it. The federal statutory scheme that this Comment proposes would be the first step in the right direction towards curbing the negative fallout from the data-broker industry.